



NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND 20755-6000

FOIA Case: 106988
21 May 2019

EMMA BEST
MUCKROCK NEWS
DEPT MR 73100
411A HIGHLAND AVE
SOMERVILLE MA 02144-2516

Dear Ms. Best:

This responds to your Freedom of Information Act (FOIA) request of 15 May 2019, which was received in the National Security Agency (NSA) FOIA office on 15 May 2019, for "Records, reports, emails, memos and other documents mentioning or relating to the Network Crack Program Hacker Group, a Chinese hacker group based out of Zigong in Sichuan Province." Your request has been assigned Case Number 106988. There are no assessable fees for this request. Your request has been processed under the FOIA.

NSA collects and provides intelligence derived from foreign communications to policymakers, military commanders, and law enforcement officials. We do this to help these individuals protect the security of the United States, its allies, and their citizens from threats such as terrorism, weapons of mass destruction, foreign espionage, international organized crime, and other hostile activities. What we are authorized to do, and how we do it, is described in Executive Order 12333. Information about how NSA conducts signals intelligence activities is available on the websites of NSA (www.nsa.gov) and the Office of the Director of National Intelligence (www.dni.gov).

To the extent that you are seeking non-intelligence records, the document you requested is enclosed. Certain information, however, has been deleted from the enclosure.

This Agency is authorized by statute to protect certain information concerning its activities, as well as the names of its employees. Such information is exempt from disclosure pursuant to the third exemption of the FOIA, which provides for the withholding of information specifically protected from disclosure by statute. The specific statute applicable in this case is Section 6, Public Law 86-36 (50 U.S. Code 3605). We have determined that such information exists in this record, and we have excised it accordingly.

In addition, certain information was withheld because it was not responsive to your request.

To the extent that you are seeking intelligence records, we have determined that the fact of the existence or non-existence of the materials you request is a currently and properly classified matter in accordance with Executive Order 13526, as set forth in Subparagraph (c) of Section 1.4. Thus, your request is denied pursuant to the first exemption of the FOIA which provides that the FOIA does not apply to matters that are specifically authorized under criteria established by an Executive Order to be kept secret in the interest of national defense or foreign relations and are, in fact properly classified pursuant to such Executive Order.

In addition, this Agency is authorized by various statutes to protect certain information concerning its activities. The third exemption of the FOIA provides for the withholding of information specifically protected from disclosure by statute. Thus, your request is also denied because the fact of the existence or non-existence of the information is exempted from disclosure pursuant to the third exemption. The specific statutes applicable in this case are Title 18 U.S. Code 798; Title 50 U.S. Code 3024(i); and Section 6, Public Law 86-36 (50 U.S. Code 3605).

You may appeal this decision. If you decide to appeal, you should do so in the manner outlined below. NSA will endeavor to respond within 20 working days of receiving any appeal, absent any unusual circumstances.

- The appeal must be sent via U.S. postal mail, fax, or electronic delivery (e-mail) and addressed to:

NSA FOIA/PA Appeal Authority (P132)
National Security Agency
9800 Savage Road STE 6932
Fort George G. Meade, MD 20755-6932

The facsimile number is 443-479-3612.

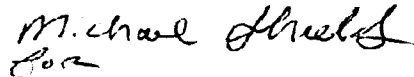
The appropriate email address to submit an appeal is
FOIARSC@nsa.gov.

- It must be postmarked or delivered electronically no later than 90 calendar days from the date of this letter. Decisions appealed after 90 days will not be addressed.
- Please include the case number provided above.
- Please describe with sufficient detail why you believe the denial of requested information was unwarranted.

You may also contact our FOIA Public Liaison at foialo@nsa.gov for any further assistance and to discuss any aspect of your request. Additionally, you may contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA mediation services they offer. The contact information for OGIS is as follows:

Office of Government Information Services
National Archives and Records Administration
8601 Adelphi Rd. - OGIS
College Park, MD 20740
ogis@nara.gov
877-684-6448
(Fax) 202-741-5769

Sincerely,

A handwritten signature in cursive script, appearing to read "Michael Shields".

JOHN R. CHAPMAN
Chief, FOIA/PA Office
NSA Initial Denial Authority

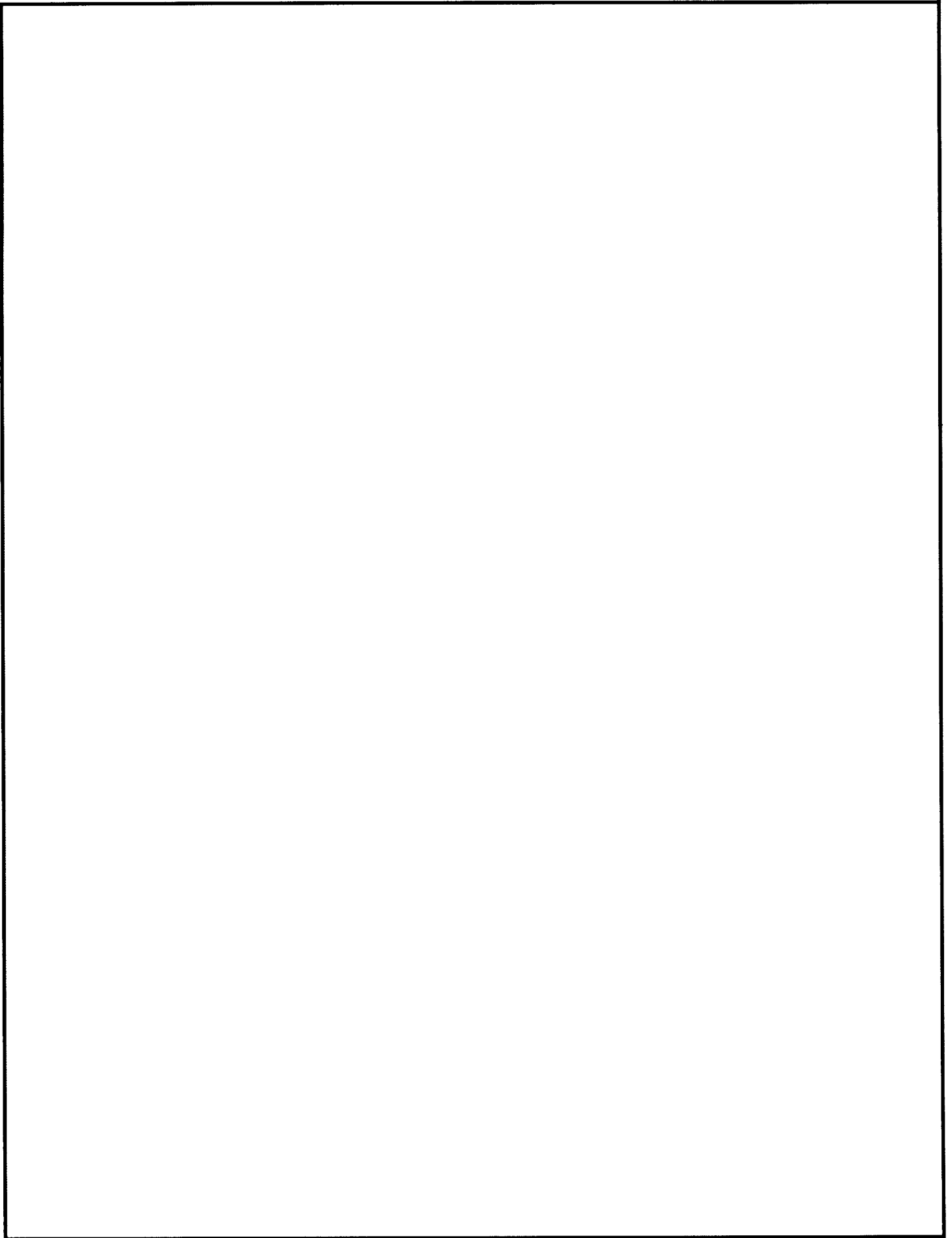
Encls:
a/s

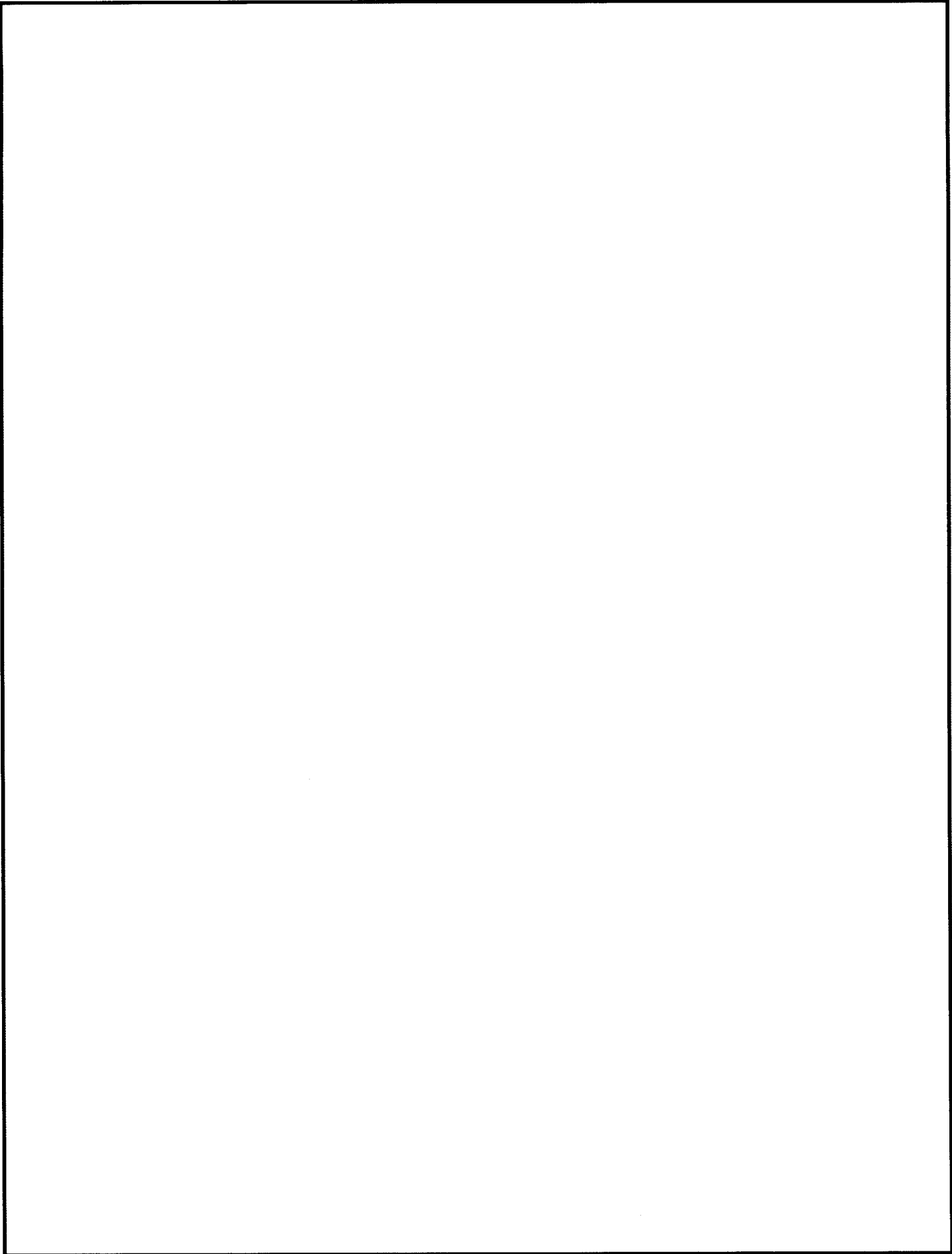
(b) (3) - P.L. 86-36

From:
Sent:
To:
Subject:

Friday, September 21, 2012 3:06 AM
Inglis John C NSA-D USA CIV
(U) Daily Pointers Daily Notification

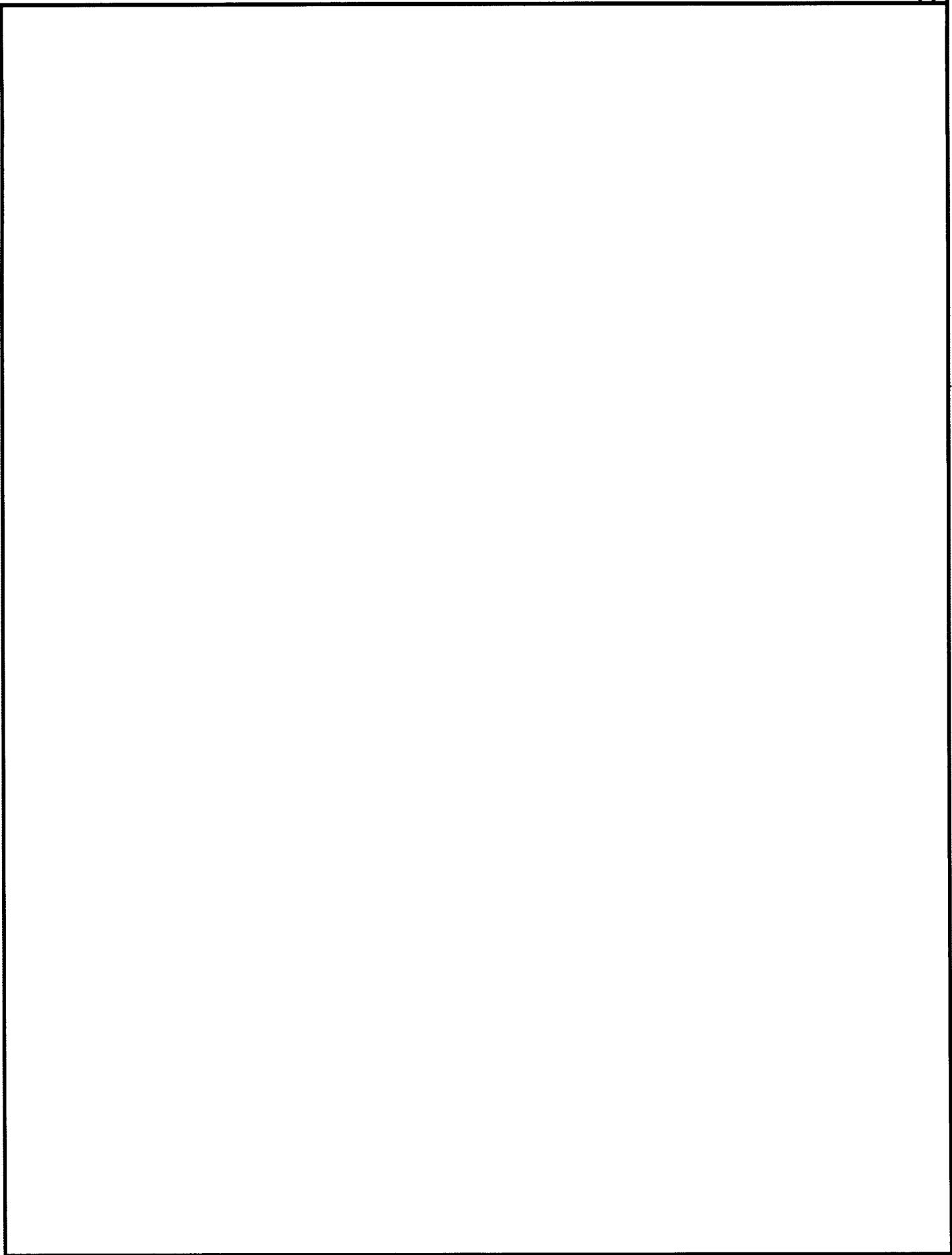
Non - Responsive

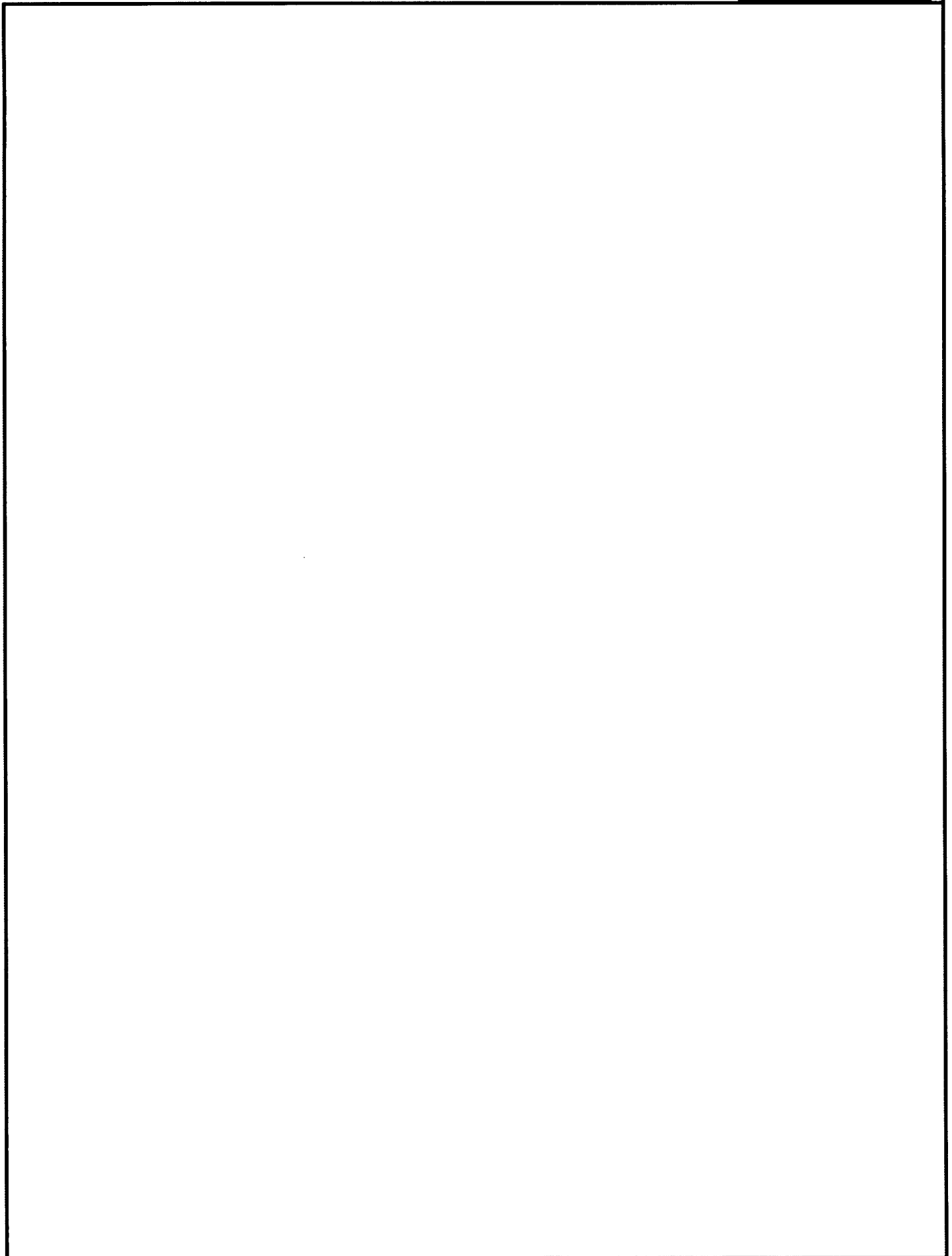


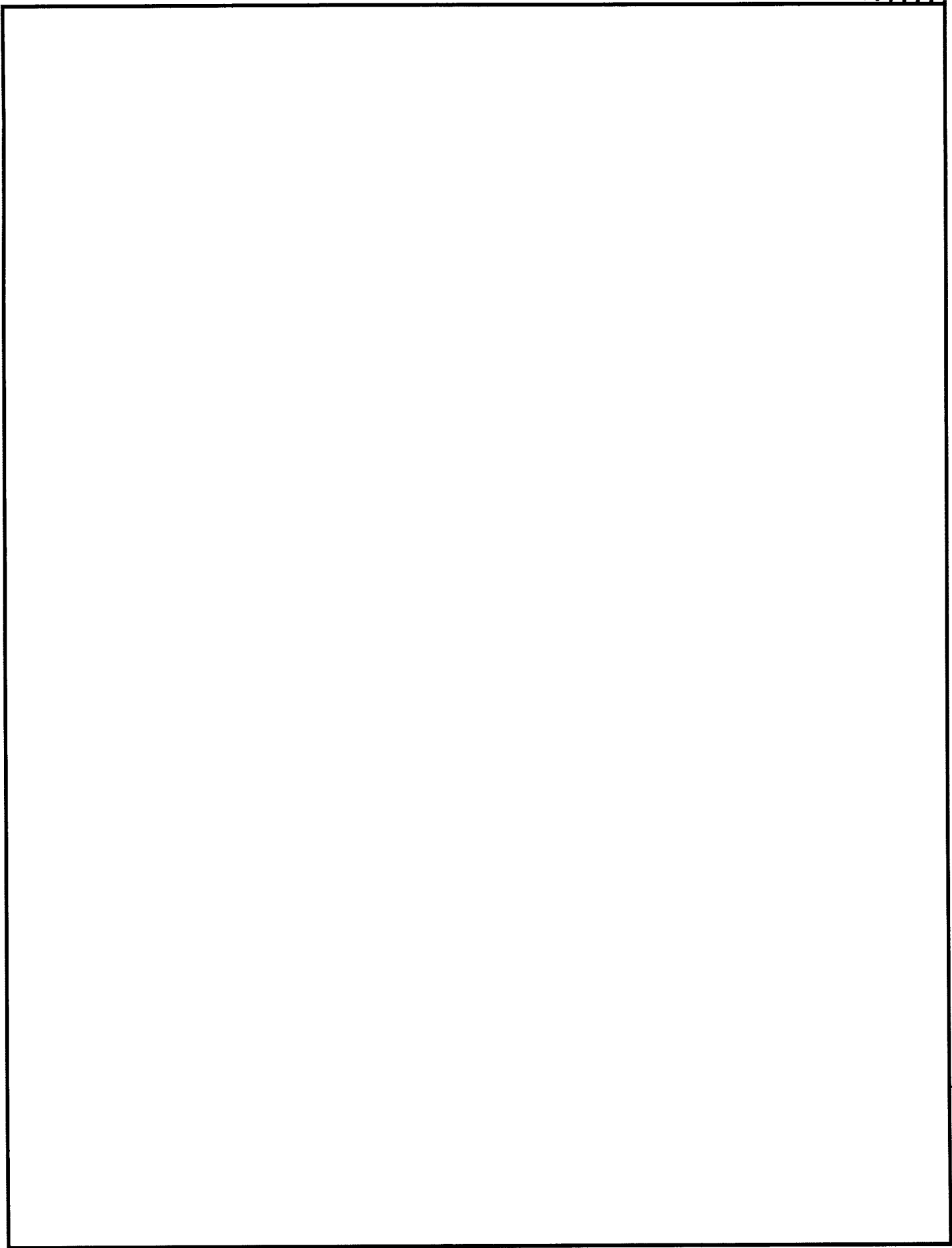


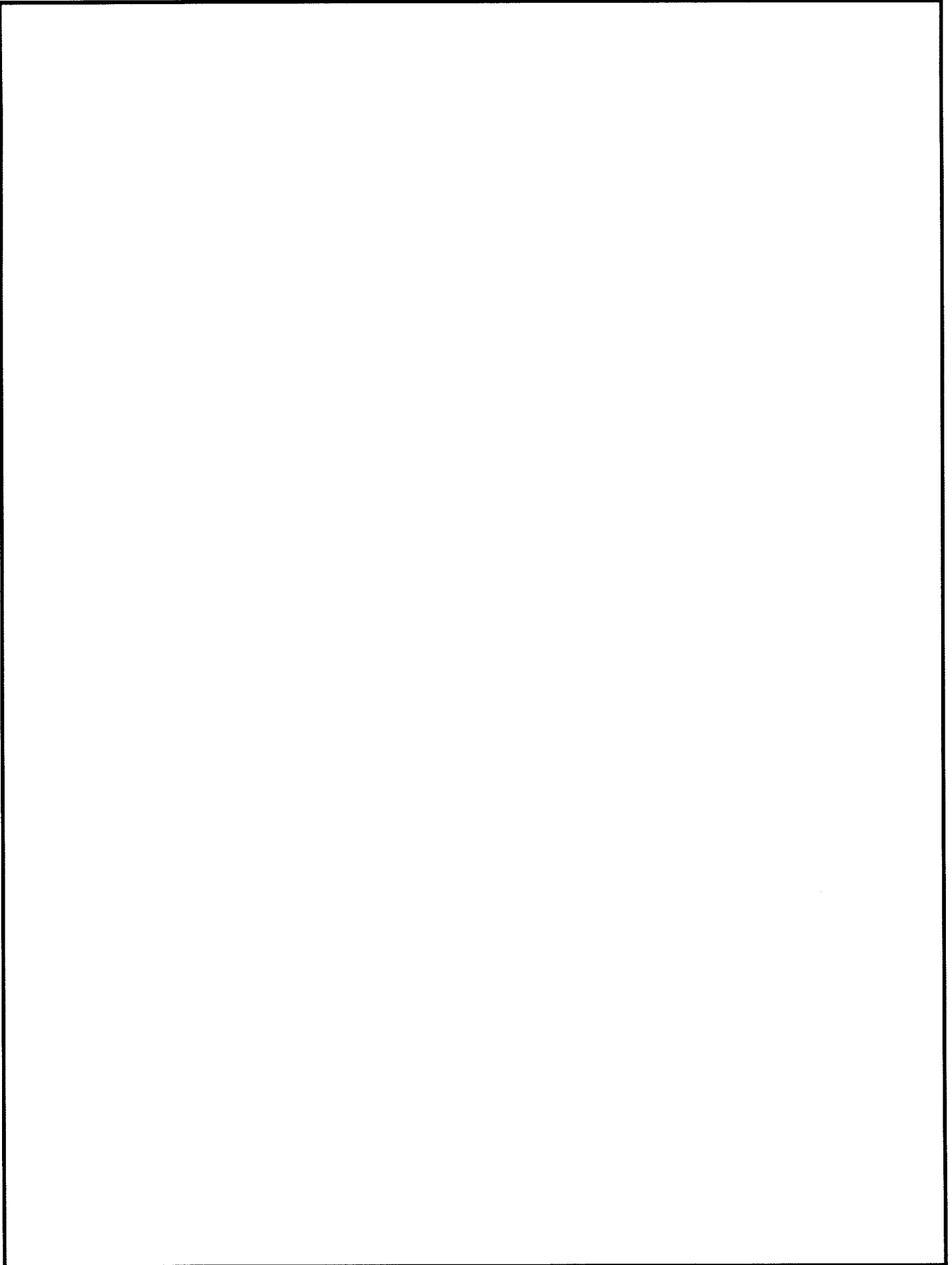
Non - Responsive

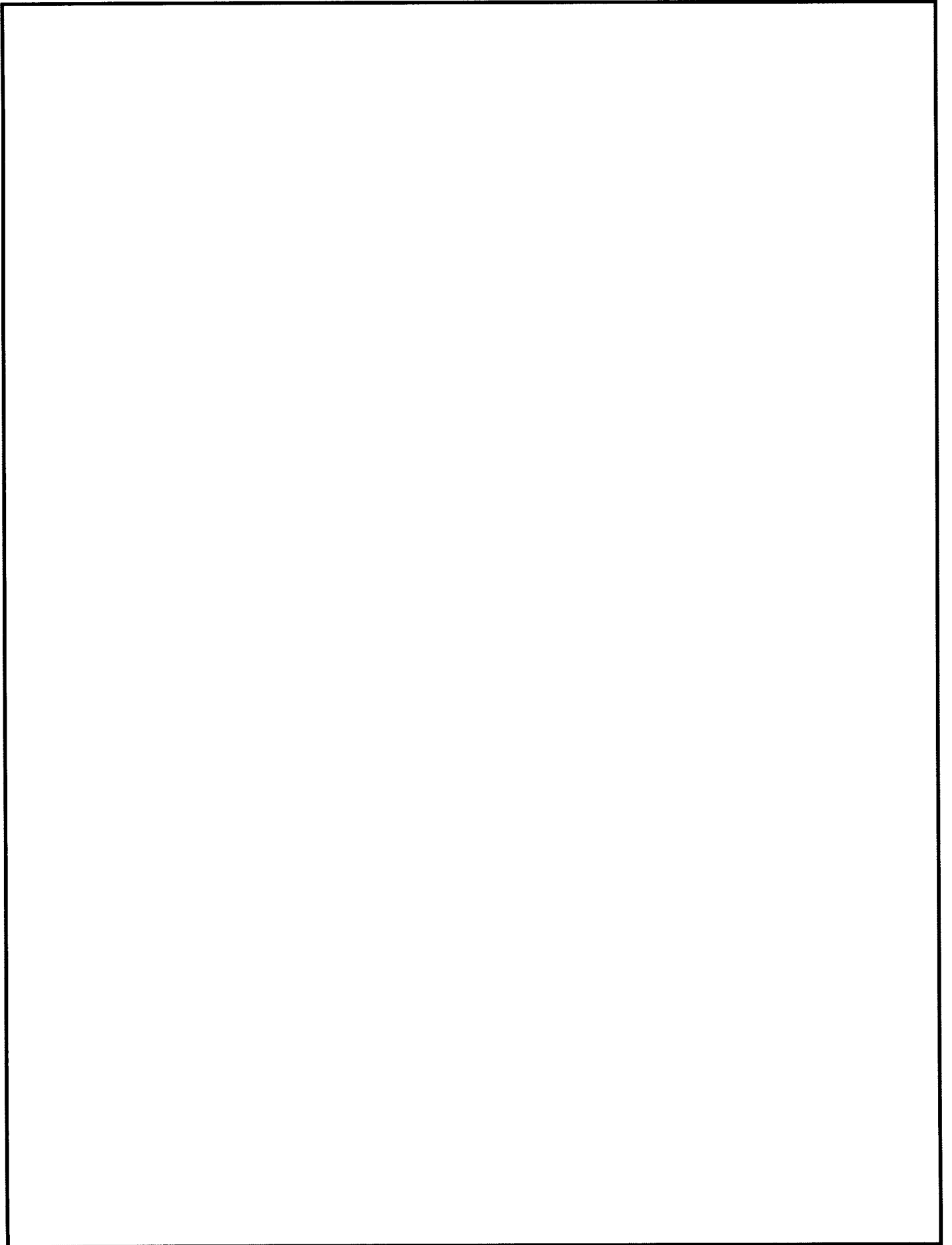
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127	128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159	160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191	192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223	224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255	256	257	258	259	260	261	262	263	264	265	266	267	268	269	270	271	272	273	274	275	276	277	278	279	280	281	282	283	284	285	286	287	288	289	290	291	292	293	294	295	296	297	298	299	300	301	302	303	304	305	306	307	308	309	310	311	312	313	314	315	316	317	318	319	320	321	322	323	324	325	326	327	328	329	330	331	332	333	334	335	336	337	338	339	340	341	342	343	344	345	346	347	348	349	350	351	352	353	354	355	356	357	358	359	360	361	362	363	364	365	366	367	368	369	370	371	372	373	374	375	376	377	378	379	380	381	382	383	384	385	386	387	388	389	390	391	392	393	394	395	396	397	398	399	400	401	402	403	404	405	406	407	408	409	410	411	412	413	414	415	416	417	418	419	420	421	422	423	424	425	426	427	428	429	430	431	432	433	434	435	436	437	438	439	440	441	442	443	444	445	446	447	448	449	450	451	452	453	454	455	456	457	458	459	460	461	462	463	464	465	466	467	468	469	470	471	472	473	474	475	476	477	478	479	480	481	482	483	484	485	486	487	488	489	490	491	492	493	494	495	496	497	498	499	500	501	502	503	504	505	506	507	508	509	510	511	512	513	514	515	516	517	518	519	520	521	5
---	---	---	---	---	---	---	---	---	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	---

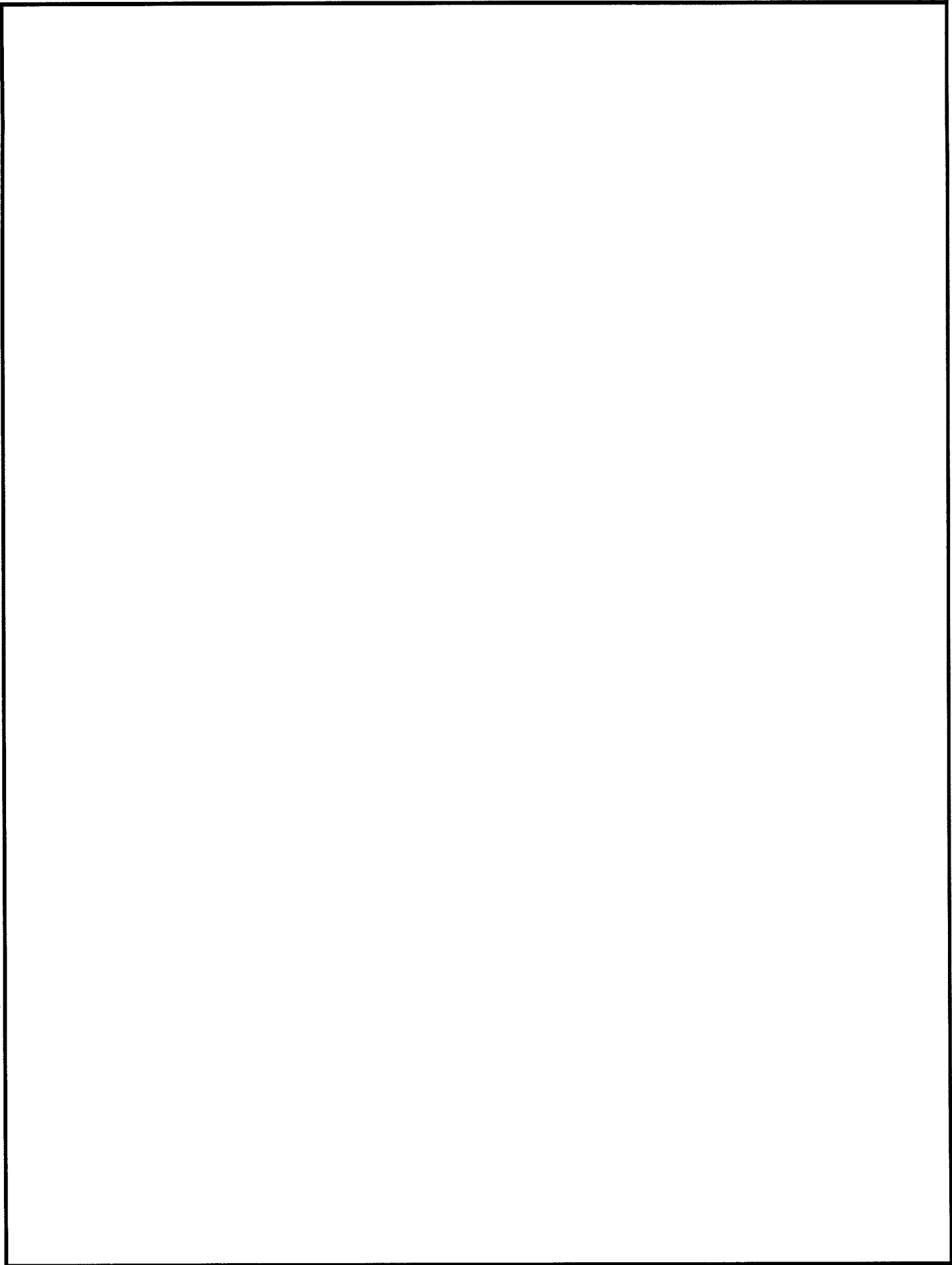


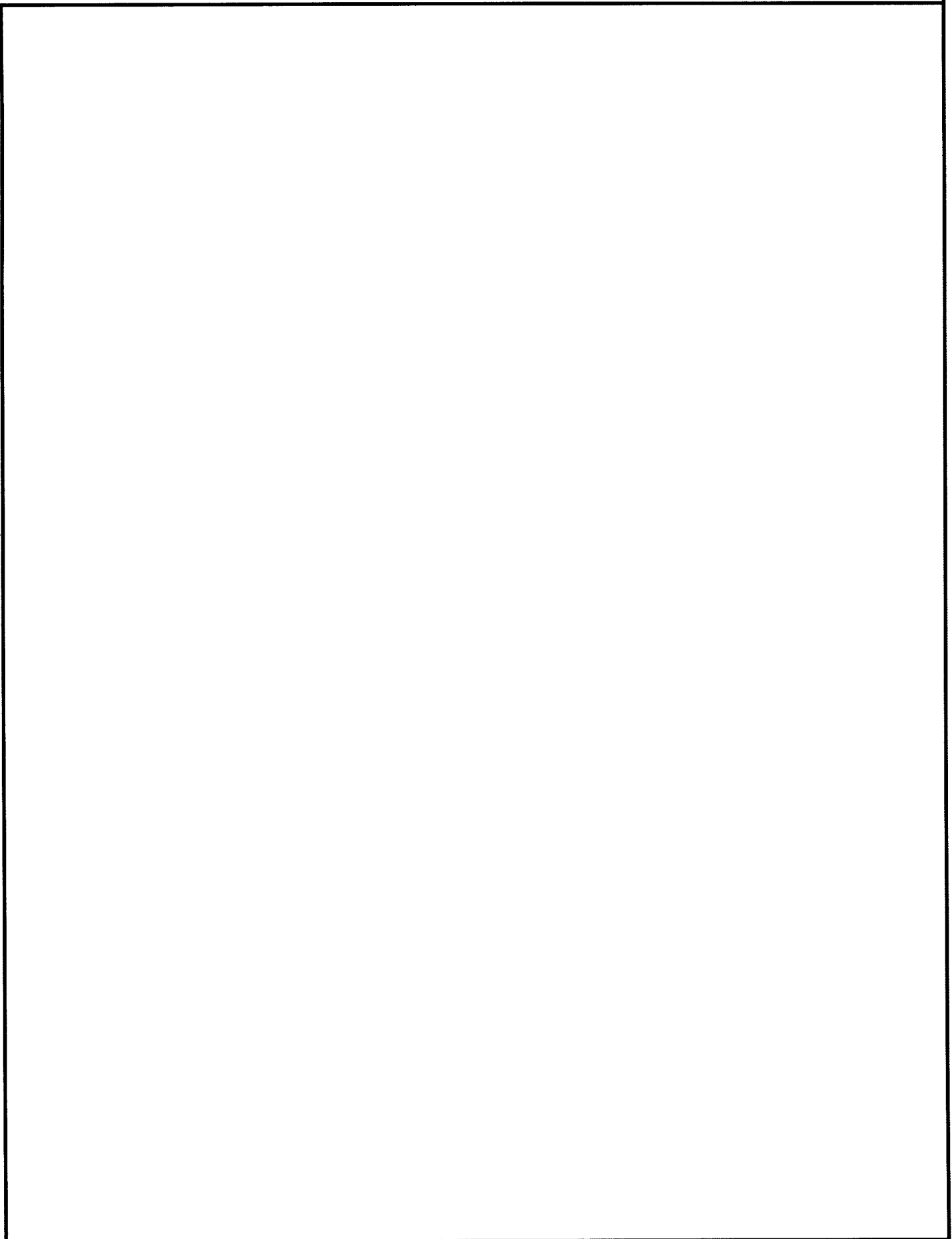


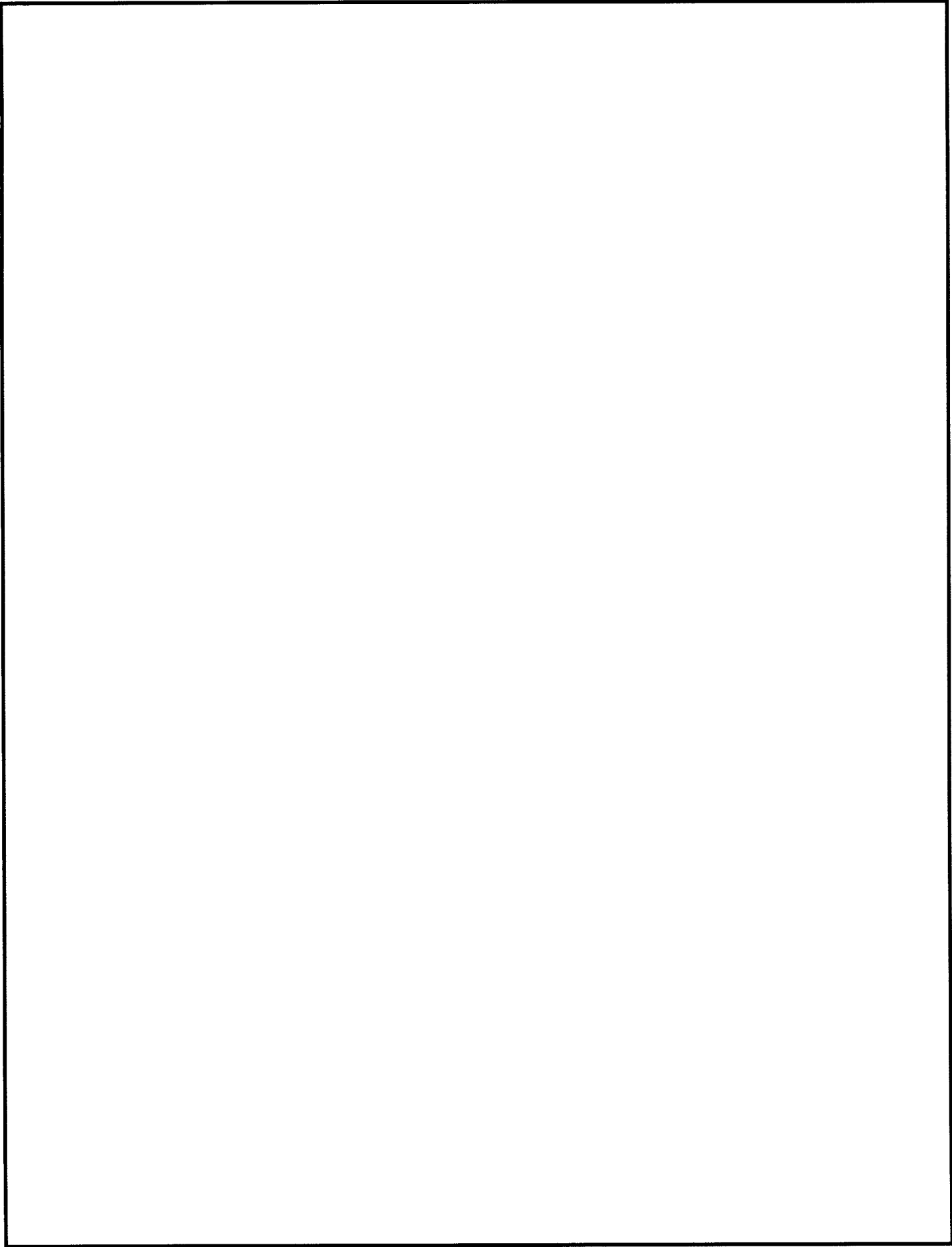


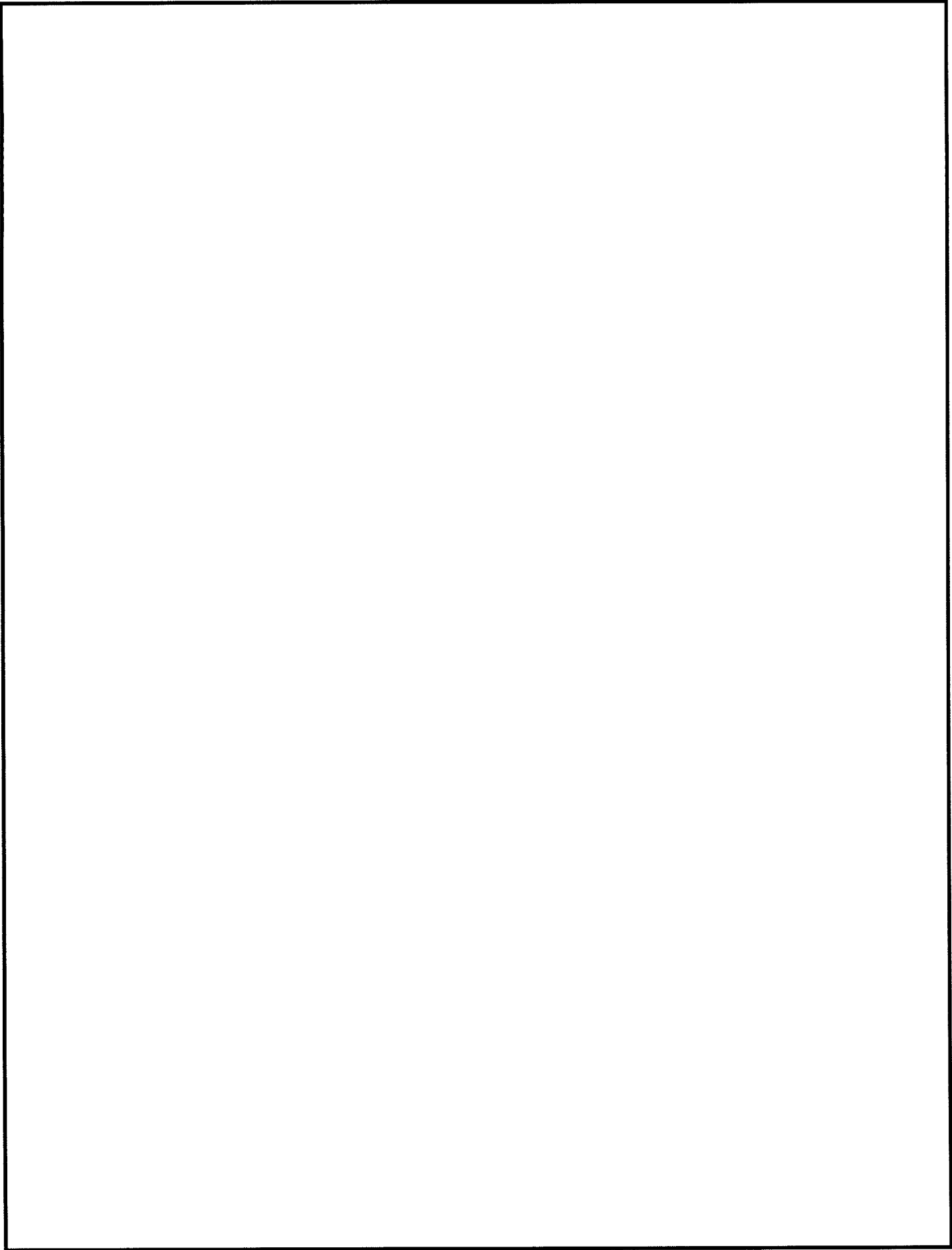






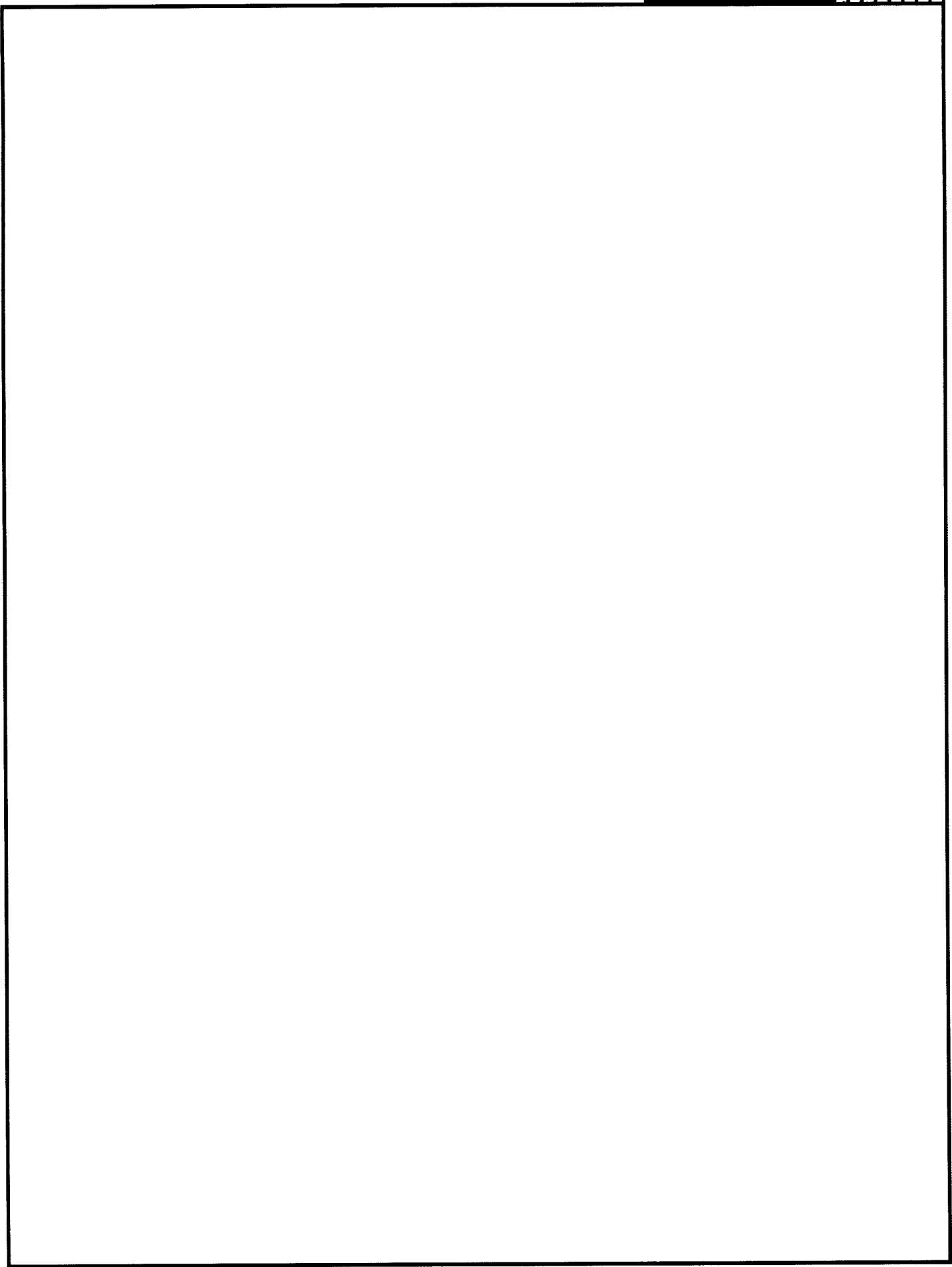




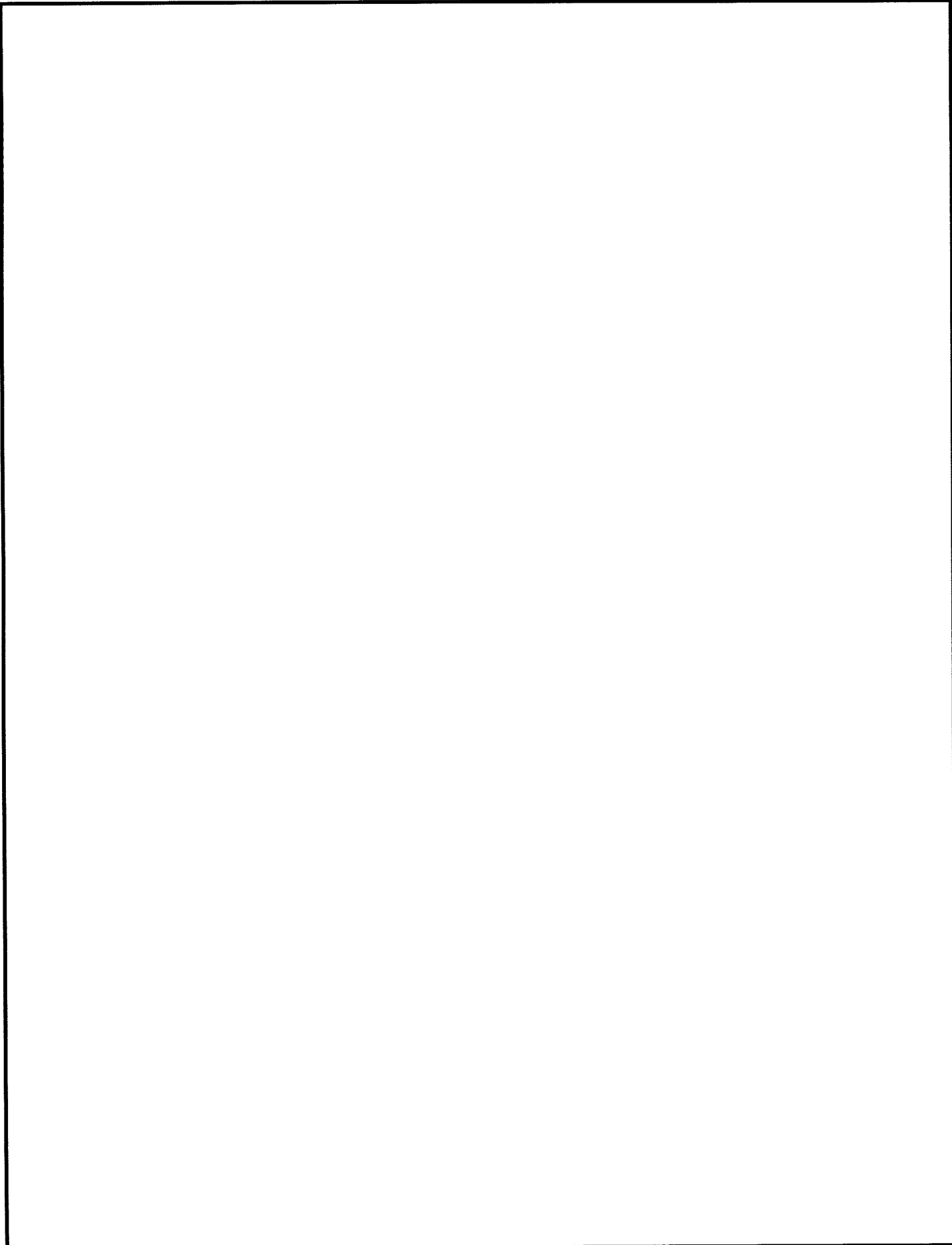


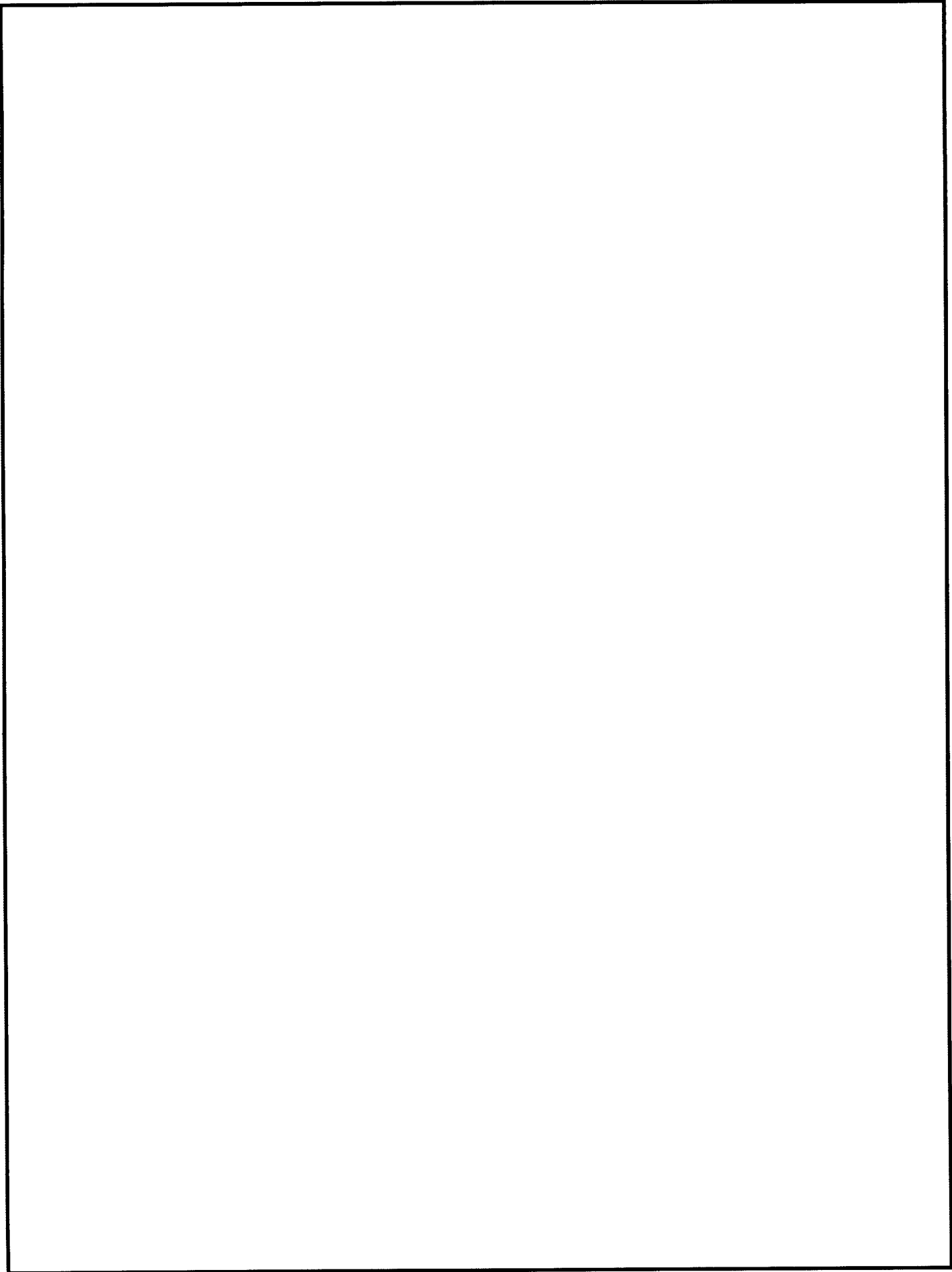
Non - Responsive

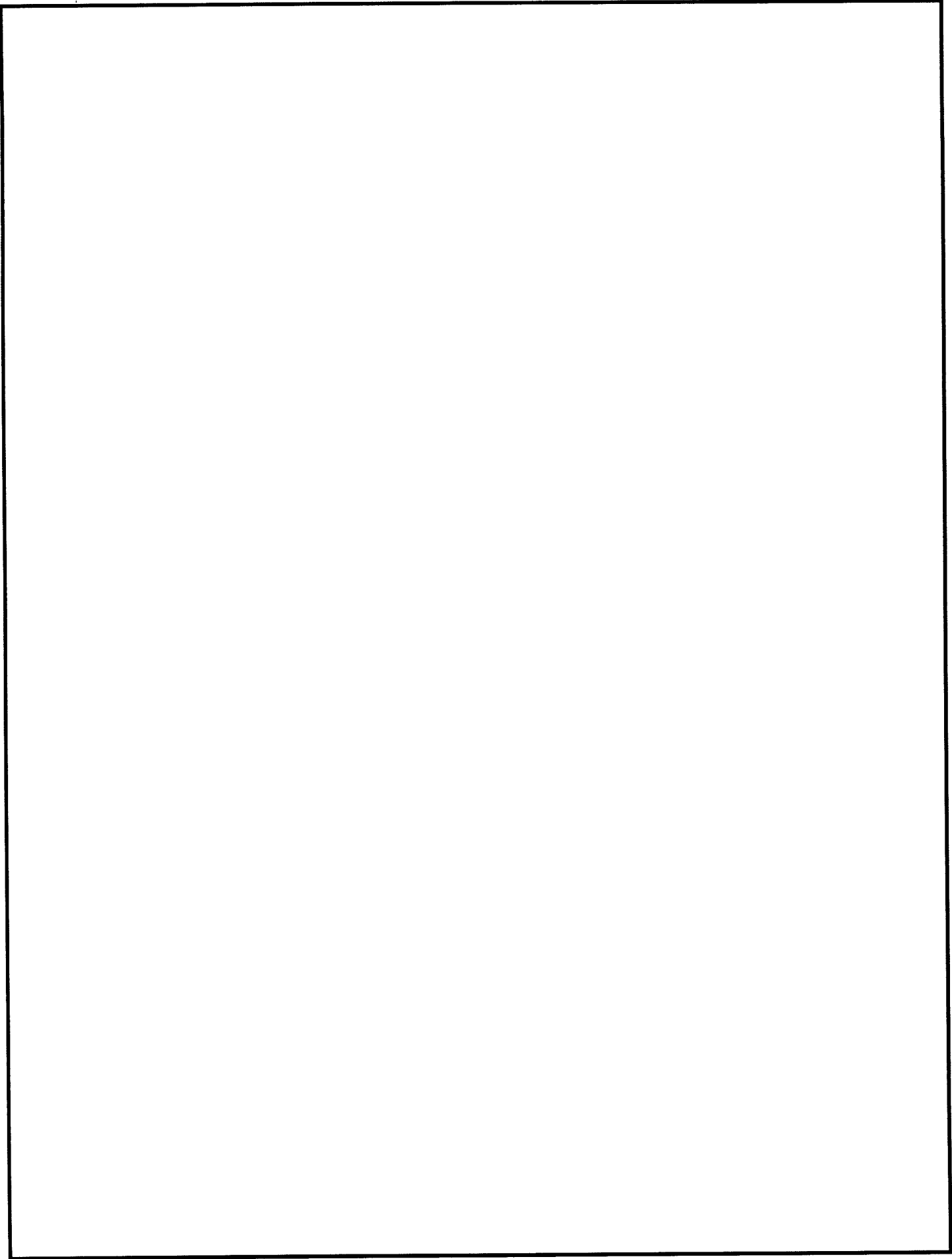
1

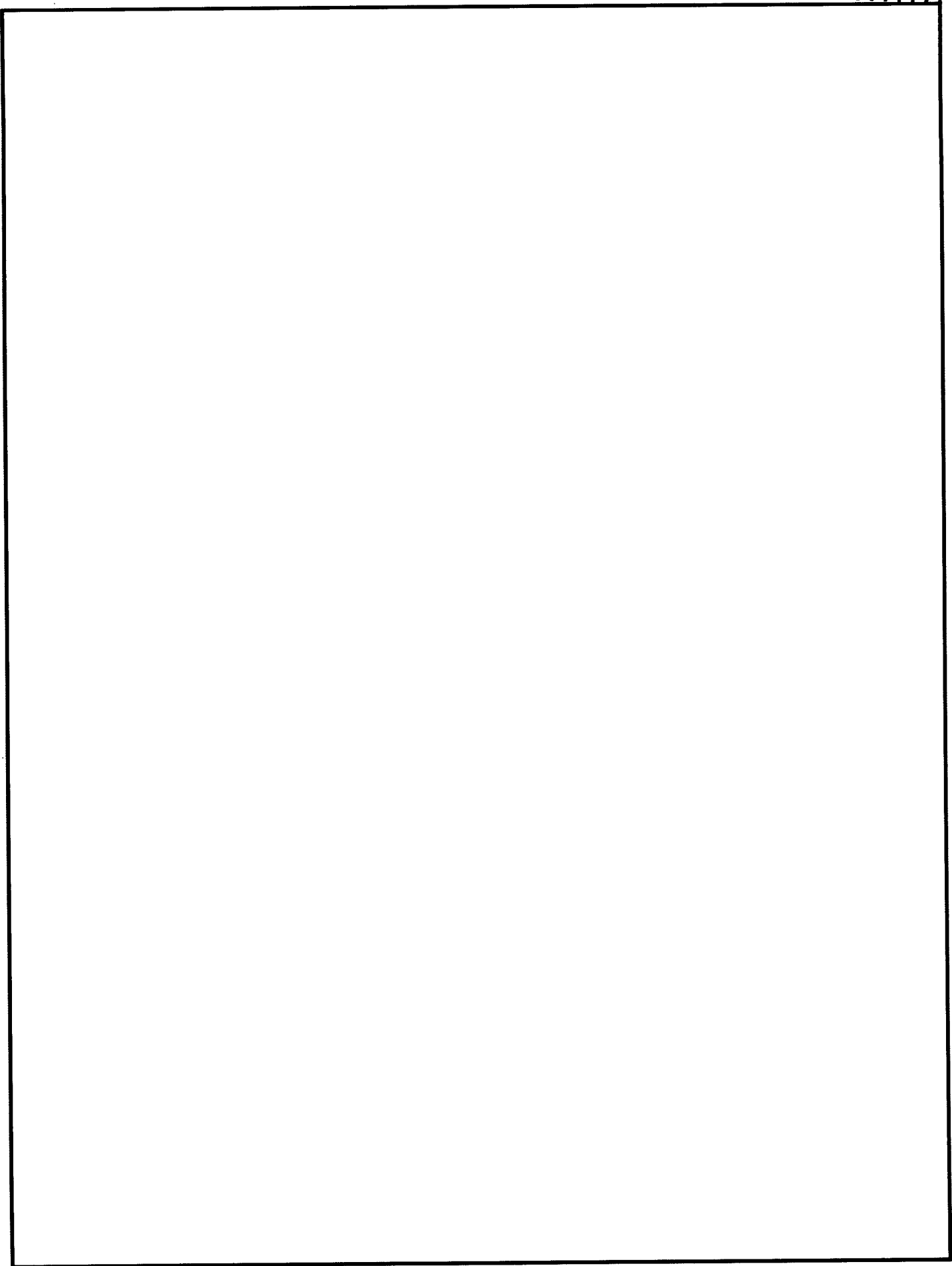


Non - Responsive

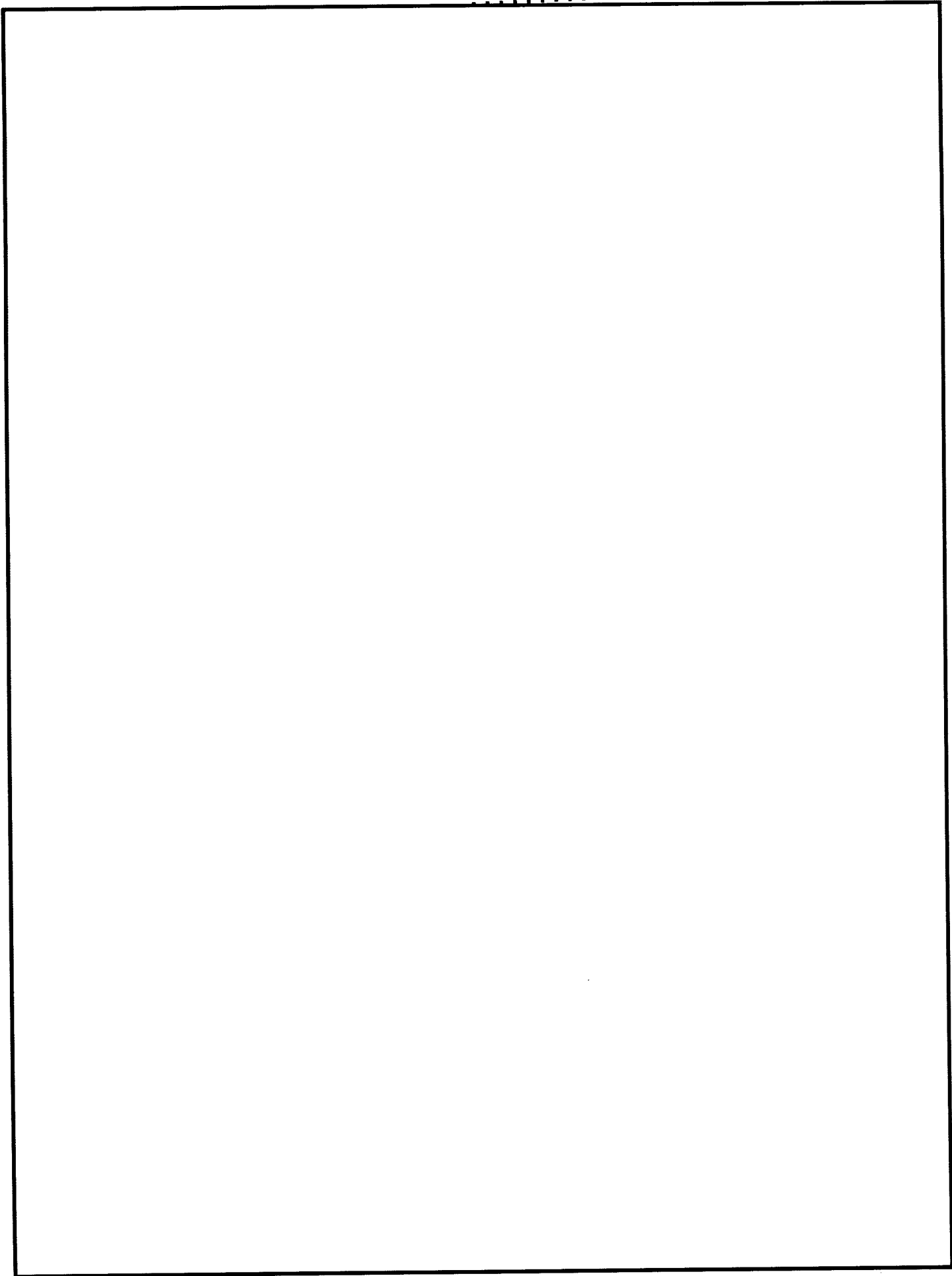


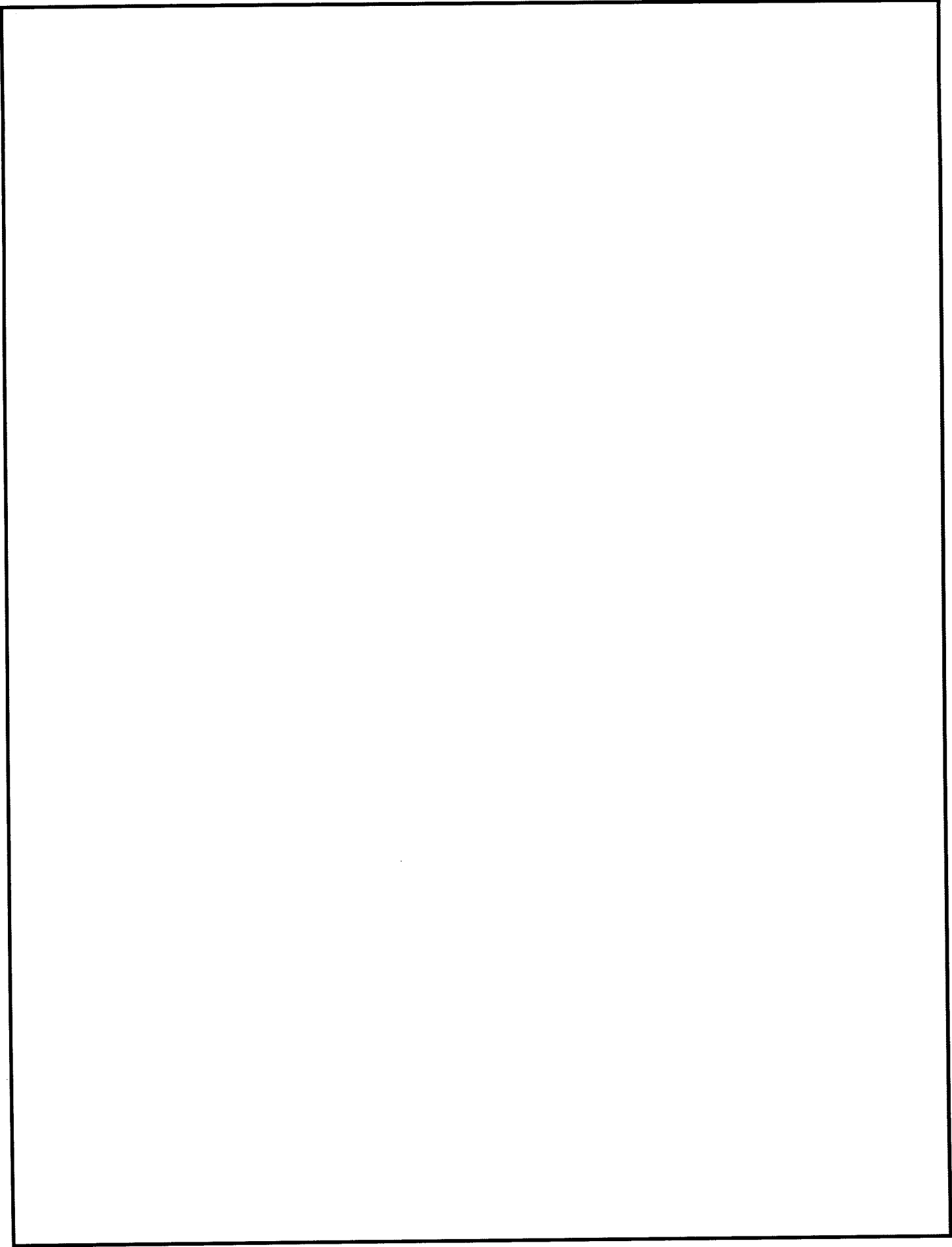






Non - Responsive





(U) New IE exploit variant distributes PlugX malware.

(U) Researchers from security vendor AlienVault have identified a variant of a recently discovered Internet Explorer exploit that is used to infect targeted computers with the PlugX remote access Trojan (RAT) program. The newly discovered exploit variant targets the same unpatched vulnerability in IE 6, 7, 8 and 9 as the original exploit, but uses slightly different code and has a different payload, AlienVault Labs manager Jaime Blasco said Tuesday in a blog post. The first exploit was found over the weekend on a known malicious server by security researcher Eric Romang and distributed the Poison Ivy RAT. The second exploit version discovered by AlienVault researchers was found on a different server and installs a much newer RAT program called PlugX. However, file modification dates seen on both servers suggest that both versions of the exploit have been in use since at least 14 September. AlienVault researchers have been tracking attacks that use the PlugX RAT since earlier this year. Based on file debug paths found inside the malware, they believe that the relatively new RAT was developed by a Chinese hacker known as WHG, who had previous ties with the Network Crack Program Hacker (NCPH), a well known Chinese hacker group. AlienVault researchers have also identified two additional websites that served the new IE exploit in the past, but no payload could be obtained from them, Blasco said. One was a defense news site from India and the other was probably a fake version of the 2nd International LED professional Symposium website, he said. "It seems the guys behind this Oday were targeting specific industries," Blasco said. The server where the original IE exploit was found also stored an exploit for an unpatched Java vulnerability last month. That Java exploit was used in attacks attributed by security researchers to a Chinese hacker group dubbed "Nitro." Microsoft already released a security advisory about the new IE vulnerability and recommended temporary mitigation solutions while it works on a patch. (IDG News Service 19Sep12)

Non - Responsive

